Network Security Exam
10/9/2020

1) Consider a message *m* encrypted with symmetric algorithm $E_K(\cdot)$ and a key *K* obtaining the ciphertext $c=E_K(m)$. What do you need for carrying out a brute force attack?

A. The ciphertext c and the encryption algorithm E(·)
B. The ciphertext c, the encryption algorithm E(·), and the key K
C. The ciphertext c, the decryption algorithm D(.), and some distinguishing mark on the cleartext m (allowing you to recognize valid plaintext messages)
D. The ciphertext c, the encryption algorithm E(·), and some distinguishing mark on the cleartext m (allowing you to recognize valid plaintext messages)
E. The ciphertext c and the decryption algorithm D(·)

2) Why a block cipher with block size equal to 16 bits cannot be considered secure?

A. because it is easy to perform a brute force attack against the secret key
B. because the encryption and decryption functions would be too fast to compute
C. because it is possible to decrypt any ciphertext, without knowing the key, after obtaining the plaintexts of 2^16 different ciphertexts.
D. because it is not possible to securely encrypt messages that are longer than 16 bits.

3) DSA is:

A. A symmetric block cipher algorithm
B. An asymmetric block cipher algorithm
C. A hash algorithm
D. A digital signature algorithm

4) What is the Euler's totient function Φ(n)?

A. The number of prime numbers lesser than *n*
B. The number of integers lesser than *n* that are relatively prime to *n*.
C. The multiplicative inverse of *n*
D. The smallest primitive root modulo *n*

5) X.509 is:

A. a symmetric cryptography algorithm
B. a digital certification standard
C. a network layer secure communication protocol that uses digital certificates
D. a transport layer secure communication protocol that uses digital certificates

6) During a TLS session setup (handshake), usually:

A. the client and the server do mutual authentication using a remote authentication (AAA) server
B. the client and the server do mutual authentication using a remote HTTPS server
C. the client sends its own X.509 certificate to the server
D. the server sends its own X.509 certificate to the client

7) List the main properties of a good cryptographic hash function.

8) Given a block cipher $E_K(\cdot)$ with block size *q* bit, show the OFB (Output Feedback) encryption mode on a message *m* with length *5*q* bit.

9) Let us consider a message *m=M1||M2||M3||M4*, and suppose to decrypt it by means of a block cipher $E_K()$ in CBC mode (the block size of $E_K()$ is equal to the size of the blocks *Mi*), with *iv=IV0*, obtaining the ciphertext *c= C1||C2||C3||C4*.
If an attacker modifies the ciphertext by rearranging the component blocks obtaining the new ciphertext c'= *C1||C4||C2||C3*, which will be the corresponding plaintext message *m'=M'1||M'2||M'3||M'4* obtained by "erroneously" decrypting the ciphertext *c'*? Show the blocks *M'i* as function of *Mj* and *Cj* with *j=1..4*.

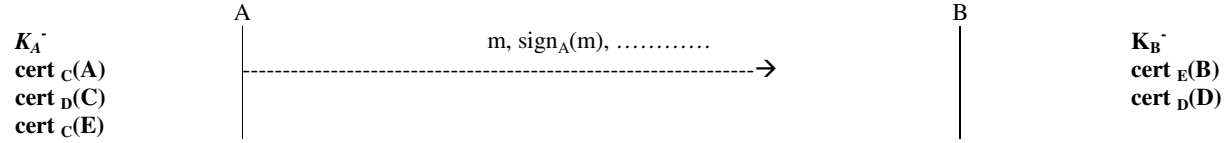
10) Create a pair of RSA public/private key pair K^+=<e,n> (public) and K^-=<d,n> (private), starting from the two secret prime numbers p=3, q=19, and value *d*=23. For obtaining the value *e* of the public key, you can either use the Euclid's algorithm or try and test knowing that *e* is lesser than 20.
By using the public key K^+ do encrypt the plaintext *m*=2.

11) Show the Diffie-Hellman exchange between Alice and Bob, using the generator g=2, the prime p=13, and the values x_A=5 and x_B=6 as secret values of Alice and Bob, respectively. Indicate the exchanges values y_A and y_B, and the resulting DH secret computed separately by Alice and Bob.

12) Show an RSA-based digital signature and verification scheme.

13) Show a possible key distribution scheme between *A* and *B* using a key distribution center KDC (For example the Needham-Schroeder Protocol or similar scheme).

14) An entity *A* wants to send a message *m* to *B* signed with her private key K_A^-. Consider that *A* has her own private key K^-_A, the $cert_C(A)$, $cert_D(C)$, and the $cert_C(E)$, while *B* has $cert_E(B)$, $cert_D(D)$. Which information should *A* add to message in order to let *B* verifying the signature?



15) The entity A wants to anonymize a message *m* to be sent to B, by using the cascade of high-latency anonymity *Mix* nodes X and Y, in such a way that A→X→Y→D is the sequence of nodes that will be involved in the delivery. Assume that K^+_i and K^-_i are the public and private keys of node *i* (with *i=A,X,Y,B*). What is a possible message that A will send to X for such a purpose?